POLYNOMIAL METHODS: RECENT ADVANCEMENTS IN COMBINATORICS

by

Thomas Fleming

A Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

Major: Mathematical Sciences

The University of Memphis

December 2021

ACKNOWLEDGMENTS

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

ABSTRACT

Fleming, Thomas Rexford. M.Sc. The University of Memphis. May 2021. Polynomial Methods: Recent Advancements in Combinatorics. Major Professor: Dr. David Grynkiewicz.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

TABLE OF CONTENTS

Contents **Pages**

Chapter 1

Introduction

Central to mathematics, the fields of Combinatorics and Number Theory seek to answer discrete problems and often employ counting arguments. Merging these fields yields Combinatorial Number Theory, also known as Additive Combinatorics. This branch of mathematics aims to prove results pertaining to sums over sequences and interpret these results to answer questions in seemingly unrelated areas. One of these methods employs a very powerful theorem from Combinatorics, the Combinatorial Nullstellensatz. This tool, and a few others collectively called the polynomial method, seek to place limits on the kernel of a particular polynomial. We begin by presenting a few results from Combinatorics that will be needed for later problems. These are generally very short proofs to prove non-obvious results.

1.1 Notation

1. For a polynomial $f\left(x_1,\ldots,x_n\right)\in R\left[x_1,\ldots,x_n\right]$ denote the coefficient of the monomial term $\prod_{i=1}^{n} x_i^{k_i}$, $k_i\in\mathbb{Z}$ to be $\left[x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}\right]f\left(x_1,\ldots,x_n\right)$. That is

$$f\left(x_1,\ldots,x_n\right)=\sum_{k_1,\ldots,k_n\in\mathbb{Z}}\left(\left[x_1^{k_1}\ldots x_n^{k_n}\right]f\left(x_1,\ldots,x_n\right)\right)x_1^{k_1}\ldots x_n^{k_n}.$$

2. For a polynomial $f\left(x_1,\ldots,x_n\right)$, we will sometimes just write $f\left(\mathbf{x}\right)$ when it is non-ambiguous.

3. We define $\deg\left(f\right)$ normally and $\deg_{x_i}\left(f\right)$ to be the degree of f in the variable x_i alone.

4.

$$\left(x\right)_0 := 1, \qquad \left(x\right)_k := \left(1-x\right)\left(1-xq\right)\left(1-xq^2\right)\ldots\left(1-xq^{k-1}\right).$$

5. Denote $(x)_k = \prod_{i=0}^{k-1} \left(1 - xq^{k-1}\right)$ for an independent variable q to be the subpower of x with respect to q. We define $(x)_0 = 1$.

1.2 Background

1. A univariate polynomial, $f : \mathbb{R} \to \mathbb{R}$ with $\deg(f) = n$ can have at most n real roots. This is a direct corollary of the Fundamental theorem of algebra.

2. jjjk

Chapter 2

Nullstellensatz

Hilbert's Nullstellensatz

Before we can approach the Combinatorial Nullstellensatz, it is important to see a closely related theorem, Hilbert's Nullstellensatz. One statement of this theorem is as follows,

Theorem 2.0.1 (Hilbert's Nullstellensatz [1])**.** Let F be an algebraically closed field and $f, g_1, \ldots, g_m \in F[x_1, \ldots, x_n]$. If for all common zeroes of $g_1, \ldots, g_m$ we find f to be zero, then there is an integer k and polynomials $h_1, \ldots, h_m \in F[x_1, \ldots, x_m]$ such that $f^k = \sum_{i=1}^{n} h_i g_i$.

We omit the proof of this theorem for now.

Add proof of Nullstellensatz

Combinatorial Nullstellensatz

Now, we move onto the main theorem of investigation, the Combinatorial Nullstellensatz. This theorem is actually a special case of Hilbert's Nullstellensatz, when $n = m$ and each g_i is a monic univariate polynomial which is zero over all of S_i. This yields a powerful generalization of the fundamental theorem of algebra. This result is applicable in proofs from graph theory, additive combinatorics, and many other branches of math. In order to prove this powerful theorem let us first state and prove the following lemma:

Lemma 2.0.1. Let R be an integral domain, $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$, and $A_1, A_2, \ldots, A_n \subseteq R$ be finite and nonempty.

Suppose $\deg_{x_i} f < |A_i|$ for each $1 \leq i \leq n$ and $f(a_1, a_2, \ldots, a_n) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$. Then f is the zero polynomial.

Proof. Let F be the quotient field of R. Clearly, any polynomial in R is a polynomial in

F and as $f = 0$ in F implies $f = 0$ in R we need only consider the case $F = R$. We will induce on n. We already know the case $n = 1$ holds by $(1.2.1)$. Now, we prove the case n. First, let us define $f_i\left(x_1, x_2, \dots, x_{n-1}\right)$ to be the non x_n component of f, that is

$$f\left(\mathbf{x}\right) = \sum_{i=0}^{\deg_{x_n} f} f_i\left(x_1, x_2, \dots, x_{n-1}\right) x_n^i.$$

We see each $f_i \in F[x_1, x_2, \dots, x_{n-1}]$ and $\deg_{x_j} f_i \leq \deg_{x_j} f \leq |A_i|$ for all $1 \leq j \leq n-1$ and $0 \leq i \leq \deg_{x_n} f$. Let $a_i \in A_i$ be an arbitrary element for each $0 \leq i \leq n-1$. As $f\left(a_1, a_2, \dots, a_{n-1}, a\right) = 0$ for all $a \in A_n$ and $\deg_{x_n} f < |A_n|$, the $n = 1$ case implies that $f\left(a_1, a_2, \dots, a_{n-1}, x_n\right) = 0$ must be the zero polynomial, hence $f_i\left(a_1, \dots, a_{n-1}\right) = 0$ for each $1 \leq i \leq n$ and each $\left(a_1, \dots, a_{n-1}\right) \in \prod_{i=1}^{n-1} A_i$. Hence, by the inductive hypothesis we must have that each f_i is the zero polynomial, and hence f is the zero polynomial. □

This lemma comprises the majority of the intellectual heavy lifting for our main theorem and hence its proof will appear very simple in comparison to its powerful statement:

Theorem 2.0.2 (Generalized Combinatorial Nullstellensatz [2])**.** Let R be an integral domain, and let $A_1, A_2, \dots, A_n \subseteq R$ be finite and nonempty.
Let $f\left(\mathbf{x}\right) \in R[x_1, x_2, \dots, x_n]$ be a polynomial and define $g_i\left(x_i\right) = \prod_{a \in A_i}\left(x_i - a\right)$ for $1 \leq i \leq n$. Then, we have that $f\left(a_1, a_2, \dots, a_n\right) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$ if and only if there are polynomials $h_1\left(\mathbf{x}\right), h_2\left(\mathbf{x}\right), \dots, h_n\left(\mathbf{x}\right) \in R[x_1, x_2, \dots, x_n]$ such that

- $f\left(\mathbf{x}\right) = \sum_{i=1}^{n} g_i\left(x_i\right)\left(h_i\left(\mathbf{x}\right)\right)$,
- $\deg\left(g_i\right) + \deg\left(h_i\right) \leq \deg\left(f\right)$ for $1 \leq i \leq n$,
- $\deg_{x_j}\left(g_i\right) + \deg_{x_j}\left(h_i\right) \leq \deg_{x_j}\left(f_i\right)$ for all $1 \leq i, j \leq n$.

Proof of Generalized Combinatorial Nullstellensatz. First, let $A_1, A_2, \dots, A_n \subseteq R$ and $f\left(\mathbf{x}\right) \in R\left[x_1, \dots, x_n\right]$ with g_i defined as in the theorem. Then, examining the backwards implication, it is clear that $f\left(\mathbf{a}\right) = 0$ for each $\mathbf{a} \in \prod_{i=1}^{n} A_i$. Now, let us examine the forwards implication . First, let $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial which is zero on the whole of such a product. We want to show that such a polynomial h_i exists for each i. For each $1 \leq j \leq n$ define g_{ji} such that

$$g_j(x_j) = \prod_{a \in A_j} (x_j - a) = x_j^{|A_j|} - \sum_{i=0}^{|A_j - 1|} g_{ji} x_j^i, \tag{2.0.1}$$

where each $g_{ji} \in R$ as well. Hence, as $a_j \in A_j$ implies that $g_j(a_j) = 0$ we must have that $a_j^{|A_j|} = \sum_{i=0}^{|A_j-1|} g_{ij} a_j^i$. Now, define $\overline{f}$ to be the polynomial for which we repeatedly apply this substitution for each j to the polynomial f. We see that $\deg_{x_i}\left(\overline{f}\right) < |A_i|$ for each i(as any monomial term of such degree can be substituted for terms of lesser degree), and as $\overline{f}(\mathbf{a}) = f(\mathbf{a}) = 0$ for each $\mathbf{a} \in \prod_{i=1}^n A_i$ (This fact is trivial by the construction of f and $\overline{f}$), then by the preceding lemma we must have that $\overline{f} = 0$. Next, consider the polynomial $f(\mathbf{x}) - \overline{f}(\mathbf{x})$. Define $f_0 = f$ and f_i to be f after the i'th such substitution. Furthermore, let $N \in \mathbb{N}$ be such that $f_N = \overline{f}$. Then, the polynomial f_i is obtained by examining a term of f_{i-1} with a degree in x_j of atleast $|A_j|$ and replacing an individual factor of $x_j^{|A_j|}$ by the sum as we defined earlier. For simplicity let us take the term $cx_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \cdot x_j^{|A_j|}$ (where $k_j \geq 0$ by our construction) and apply such a substitution. Then, we see that the difference

$$f_{i-1} - f_i = cx_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \left(x_j^{|A_j|} - \sum_{i=0}^{|A_j|-1} g_{ji} x_j^i \right) = cx_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \cdot g_j(x_j)$$

by our original definition. Furthermore, as $f_N = \overline{f}$ we have that

$$f - \overline{f} = (f_0 - f_1) + (f_1 - f_2) + \ldots + (f_{N-1} - f_N).$$

Hence, $f = f - 0 = f - \overline{f} = \sum_{j=1}^n g_j(x_j) h_j$ where each $h_j \in R[x_1, x_2, \ldots, x_n]$ is simply the sum of all of these preceding terms $cx_1^{k_1} \ldots x_n^{k_n}$ as a result of these substitutions.

Furthermore, by construction we had that $\deg g_j = |A_j| > \deg\left(\sum_{i=0}^{|A_j|-1} g_{ji}x_j^i\right)$, so we see that such a substitution will never increase the degree of our polynomial and hence $\deg f_i \leq \deg f$. Then, as $\deg g_j = |A_j|$ we see that

$$\deg\left(cx_1^{k_1}\ldots x_n^{k_n} g_j(x_j)\right) \leq \deg f_{i-1} \leq \deg f.$$

Using the additive nature of polynomial degree yields $\deg\left(cx_1^{k_1}\ldots x_n^{k_n}\right) + \deg g_j \leq \deg f$, and as each h_j is simply the sum of such terms we may substitute its degree to yield $\deg g_j + \deg h_j \leq \deg f$.

Lastly, we show this holds for projected degree as well. Note that as we are replacing a term, g_j with $\deg_{x_k}(g_j) = 0$ and as each h_j with $\sum_{i=0}^{|A_j|-1} g_{ji}x_j^i$, also having projected degree 0, the overall degree in x_k will not change after i substitutions. Hence, $\deg_{x_k}\left(cx_1^{k_1}\ldots x_n^{k_n} g_j(x_j)\right) = \deg_{x_k}(f_{i-1}) = \deg_{x_k}(f)$. This yields $\deg_{x_k}\left(cx_1^{k_1}\ldots x_n^{k_n}\right) + \deg_{x_k}(g_j) = \deg_{x_k}(f)$. And, as each h_j is simply the sum of these remaining terms, we see $\deg_{x_k}(h_j) + \deg_{x_k}(g_j) \leq \deg_{x_k}(f)$ for each $1 \leq j, k \leq n$. □

This theorem is perhaps too general and too powerful for use in proving our simpler results. As a corollary, many authors include a weaker second statement of the theorem, where the splitting of a polynomial is replaced by a constraint on the size of the kernel.

Theorem 2.0.3 (Combinatorial Nullstellensatz [2])**.** Let R be an integral domain, with $A_1, A_2, \ldots, A_n \subseteq R$ being finite and nonempty, and $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ being a polynomial. Suppose

$$[x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}] f(\mathbf{x}) \neq 0$$

and that $\deg f = \sum_{i=1}^{n} d_i$ with $0 \leq d_i \leq |A_i| - 1$. Then, there exists an element $\mathbf{a} \in \prod_{i=1}^{n} A_i$ such that $f(\mathbf{a}) \neq 0$. That is, given a nontrivial "maximal degree" monomial of f such that the degree of this monomial in each variable individually is strictly less than the size of the corresponding set A_i, f cannot be zero on the whole of the product of the A_i.

This is the generalization of the Fundamental theorem of Algebra to which we referred earlier and it is precisely this simple statement about the size of the kernel of a particular polynomial which provides our combinatorial power. The proof follows rather directly from the negation of the generalized version and it is as follows:

Proof. Let $g_i = \prod_{a \in A_i} (x_i - a)$ for $1 \leq i \leq n$ and suppose the contrary. That is, $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$ despite the assumptions of the construction. Then, applying the generalized combinatorial nullstellensatz yields polynomials $h_1, h_2, \ldots, h_n \in R[x_1, x_2, \ldots, x_n]$ with the desired properties. Now let us examine the nature of $[x_1^{d_1} \ldots x_n^{d_n}] f(\mathbf{x})$. As this is a maximal degree monomial of f, then only maximal degree monomials of $h_i(\mathbf{x}) \, g_i(x_i)$ can contribute to its coefficient in f as $\deg(h_i) + \deg(g_i) = \deg h_i g_i \leq \deg f$. However, by the construction of g_i, all such monomials will be taken from the $h_i(\mathbf{x}) \cdot x_i^{|A_i|}$ portion of this polynomial. Thus $\deg_{x_i} h_i g_i > d_i$ by our requirement that each $d_i < |A_i|$, hence all maximal degree monomials of f must be of the form $x_1^{k_1} x_2^{k_2} \ldots x_j^{|A_j|} \ldots x_n^{k_n}$. Thus, we must have $[x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}] f(\mathbf{x}) = 0$, ↯. Hence, there must be an $\mathbf{a} \in \prod_{i=1}^{n} A_i$ such that $f(\mathbf{a}) \neq 0$. □

Our last version of the Combinatorial Nullstellensatz will examine what happens when f vanishes over not all, but most (in a certain set-theoretic perspective) of the members of the product. This is known as the Punctured Combinatorial Nullstellensatz and it builds on the original generalized version. The proof will involve division of polynomials of many variables, so let us first examine the nature of such an operation.

Punctured Nullstellensatz

Sometimes we will not have polynomials which are zero over the whole of a set, but just on part. These conditions yield the Punctured Nullstellensatz. But, before we may state the theorem itself, we must state a result about the well-behavedness of multivariate polynomial division.

Lemma 2.0.2 (Multivariate Polynomial Division [2])**.** Let R be an integral domain and let $g_1\left(x_1\right), \ldots, g_k\left(x_k\right) \in R[x_1, x_2, \ldots, x_n]$ be polynomials of one variable with leading coefficient 1 for $1 \leq k \leq n$. Then,

1. If $f \in \sum_{i=1}^{k} R\left[x_1, \ldots, x_n\right] \cdot g_i\left(x_i\right)$ is a nonzero polynomial in the ideal generated by $g_1\left(x_1\right), \ldots, g_k\left(x_k\right)$ over $R\left[x_1, \ldots, x_n\right]$, then $\deg_{x_i}\left(f\right) \geq \deg\left(g_i\right)$ for some $1 \leq i \leq k$.

2. For a polynomial $f \in R\left[x_1, \ldots, x_n\right]$ there are $w\left(\mathbf{x}\right), h_1\left(\mathbf{x}\right), \ldots, h_k\left(\mathbf{x}\right) \in R\left[x_1, \ldots, x_n\right]$ such that all of the following hold :

   - $f\left(\mathbf{x}\right) = \sum_{i=1}^{k} h_i\left(\mathbf{x}\right) g_i\left(x_i\right) + w\left(\mathbf{x}\right)$.
   - $\deg_{x_j}\left(w\right) < \deg\left(g_j\right)$ for $1 \leq j \leq k$,
   - $\deg_{x_j}\left(g_i\right) + \deg_{x_j}\left(h_i\right) \leq \deg_{x_j}\left(f\right)$ for $1 \leq i \leq k$, $1 \leq j \leq n$,
   - $\deg\left(g_i\right) + \deg\left(h_i\right) \leq \deg\left(f\right)$ for $1 \leq i \leq k$,
   - $\deg_{x_i}\left(w\right) \leq \deg_{x_i}\left(f\right)$ for $1 \leq i \leq n$,
   - $\deg\left(w\right) \leq \deg\left(f\right)$.

Furthermore, the polynomial $w\left(\mathbf{x}\right)$ is unique .

Proof. First, we show the existence of the first condition of 2. We see each g_j so we use a similar strategy to the Combinatorial Nullstellensatz. Let $g_{ji} \in R$ such that $g_j\left(x_j\right) = x_j^{\deg(g_j)} - \sum_{i=0}^{\deg(g_j)-1} g_{ji} x_j^i$. Fix j such that $\deg_{x_j}\left(f\right) \geq \deg\left(g_j\right)$. Then, we may write $f\left(\mathbf{x}\right)=A\left(\mathbf{x}\right)x_j^{\deg\left(g_j\right)}+B\left(\mathbf{x}\right)$, where $A,B\in R\left[x_1.\ldots,x_n\right]$ and $\deg_{x_j}\left(B\right)<\deg\left(g_j\right)$ and $\deg\left(g_j\right)+\deg\left(A\right)\leq\deg\left(f\right)$ and $\deg_{x_i}\left(Ax_j^{\deg\left(g_j\right)}\right)\leq\deg_{x_i}\left(f\right)$. Substituting g_j yields

$$f\left(\mathbf{x}\right)=A\left(\mathbf{x}\right)g_j\left(x_j\right)+A\left(\mathbf{x}\right)\sum_{i=0}^{\deg\left(g_j\right)-1}g_{ji}x_j^i+B\left(\mathbf{x}\right).$$

Letting $f_1=A\left(\mathbf{x}\right)\sum_{i=0}^{\deg\left(g_j\right)-1}g_{ji}x_j^i+B\left(\mathbf{x}\right)$ yields $\deg_{x_i}\left(f_1\right)\leq\deg_{x_i}\left(f\right)$ for all $1\leq i\leq j$ and $\deg_{x_i}\left(f_1\right)<\deg_{x_i}\left(f\right)$ for $i=j$. Furthermore, $\deg\left(f_1\right)<\deg\left(f\right)$. Now, we define $f_1\left(\mathbf{x}\right)=A_1\left(\mathbf{x}\right)g_k\left(x_k\right)+A\left(\mathbf{x}\right)\sum_{i=0}^{\deg\left(g_k\right)-1}g_{ki}x_k^i+B_1\left(\mathbf{x}\right)$ and we continue this procedure over all x_j. Then, we find

$$f\left(\mathbf{x}\right)=\sum_{i=1}^{k}h_i\left(\mathbf{x}\right)g_i\left(x_i\right)+w\left(\mathbf{x}\right)$$

□

Theorem 2.0.4 (Punctured Combinatorial Nullstellensatz [2])**.** Let R be an integral domain and let $A_1, A_2, \ldots, A_n \subset R$ be finite and nonempty. Furthermore, for each $1 \leq i \leq n$ let $B_i \subseteq A_i$ be nonempty.

Let $f\left(\mathbf{x}\right) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial and set $g_i\left(x_i\right) = \prod_{a \in A_i}\left(x_i - a\right)$ and $l_i\left(x_i\right) = \prod_{b \in B_i}\left(x_i - b\right)$. If

$$f\left(\mathbf{a}\right) = 0 \, \forall \, \mathbf{a} \in \left(\prod_{i=1}^{n} A_i\right) \setminus \left(\prod_{i=1}^{n} B_i\right) \tag{2.0.2}$$

but there exists a $\mathbf{b} \in \prod_{i=1}^{n} B_i$ such that $f\left(\mathbf{b}\right) \neq 0$ then there are polynomial $h_i \in R[x_1, x_2, \ldots, x_n]$ with $1 \leq i \leq n$ such that

$$f\left(\mathbf{x}\right) = \sum_{i=1}^{n} g_i\left(x_i\right) h_i\left(\mathbf{x}\right) + w\left(\mathbf{x}\right) \text{ with } w\left(\mathbf{x}\right) = u\left(\mathbf{x}\right) \prod_{i=1}^{n} \frac{g_i\left(x_i\right)}{l_i\left(x_i\right)}.$$

with the following conditions holding:

$\deg\left(w\right) \leq \deg\left(f\right) \deg_{x_j}\left(w\right) \leq \deg_{x_j}\left(f\right)$ for all $1 \leq j \leq n$, $\deg_{x_i}\left(w\right) < |A_i|$, $\deg\left(g_i\right) + \deg\left(h_i\right) \leq \deg\left(f\right)$ for $1 \leq i \leq n$ and

$\deg_{x_j}\left(g_i\left(x_i\right)\right) + \deg_{x_j}\left(h_i\right) \leq \deg_{x_j}\left(f\right)$ for $1 \leq i, j \leq n$. Consequently $\sum_{i=1}^{n}\left(|A_i| - |B_i|\right) \leq \deg\left(w\right) \leq \deg\left(f\right)$.

Proof. The preceding lemma guarantees there to be polynomials

$$w\left(\mathbf{x}\right), h_1\left(\mathbf{x}\right), \ldots, h_n\left(\mathbf{x}\right) \in R[x_1, x_2, \ldots, x_n]$$

of the desired form and for which the proper conditions hold (case 2). Our task, then, is to ensure that the form of $w\left(\mathbf{x}\right)$ is that of our statement. First, let $1 \leq i \leq n$ and without loss of generality select $i = 1$. First, we consider $w\left(\mathbf{x}\right) l_1\left(x_1\right)$. Then as f and the first sum of equation (2) must be zero on all $\mathbf{a} \in \prod_{i=1}^{n} A_i \setminus \prod_{i=1}^{n} B_i$, we see $w\left(\mathbf{x}\right)$ must also vanish on this difference of products. Furthermore, by the construction of l_1 we must have that

$w(\mathbf{x})\,l_1(x_1)$ vanishes on $\prod_{i=1}^{n} B_i$ as well, hence it vanishes on all of $\prod_{i=1}^{n} A_i$. Applying theorem 1 (Generalized Combinatorial Nullstellensatz) yields polynomials $v_1, \ldots, v_n \in R[x_1, \ldots, x_n]$ such that

$$w(\mathbf{x})\,l_1(x_1) = \sum_{i=1}^{n} g_i(x_i)\,v_i(\mathbf{x}). \tag{2.0.3}$$

Now, by the preceding lemma we may assume that $v_j(\mathbf{x})$ is not of the form in case 1. Furthermore, for $n > 1$, we see $\deg_{x_n}(w(\mathbf{x})\,l_i(x_i)) > |A_n|$ as a consequence of the stipulations of $w(\mathbf{x})$. Now, for a polynomial $h \in f[x_1, ..., x_n]$ define $\overline{h}$ to be h reduced modulo the ideal generated by $g_1(x_1), \ldots, g_{n-1}(x_{n-1})$. Applying this operation to equation (4) yields

$$\overline{w(\mathbf{x})\,l_1(x_1)} = \overline{g_n(x_n)\,v_n(\mathbf{x})}.$$

□

Finish Proof of Punctured Nullstellensatz

With all three variations of the Combinatorial Nullstellensatz fully stated and proven, allow us to move on to the examination of some of the most powerful results which these theorems prove, namely in combinatorics. We will begin with a proof of the Chevalley-Warning theorem as well as several results of additive combinatorics concerning sumsets, both standard and restricted.

Maybe change proof to the one found in Simeon and Ball

Chapter 3

Simple Combinatorial Proofs

3.1 Sumsets

prove 1-2 more combinatorial statements with Nullstellensatz

Now, with our the Nullstellensatz stated and proven, let us examine a few simple results concerning sumsets, those being the pointwise sum of all coordinates

Theorem 3.1.1 (Cauchy-Davenport Theorem [1])**.** Given a prime p and nonempty $A, B \subseteq Z_p$, then $|A+B| \geq \min\{p, |A|+|B|-1\}$.

Proof. Suppose $|A|+|B|>p$, we must have that for any element $x \in Z_p$, $(A) \cap (x \setminus B) \neq \varnothing$ (As there are only p possible elements which could be in each set). Hence, $A+B=Z_p$. Thus, let us assume $|A|+|B| \leq p$ and suppose indirectly that $|A+B| \leq |A|+|B|-2$. Let $A+B \subseteq C \subseteq Z_p$ such that $|C|=|A|+|B|-2$. Next, define $f(x,y)=\prod_{c\in C}(x+y-c)$ and note that we must have $f(a,b)=0$ for all $(a,b)\in A\times B$ as $A,B\subseteq C$. Now, note that $\deg(f)=|C|=|A|+|B|-2$, and hence $[x^{|A|-1}y^{|B|-1}]f(x,y)=\binom{|A|+|B|-2}{|A|-1}\neq 0$ as $|A|-1<|A|+|B|-2<p$. Hence, by the Combinatorial Nullstellensatz (Theorem 1.2), we must have a pair $(a,b)\in A\times B$ such that $f(a,b)\neq 0$ $\lightning$. Thus, the theorem must be true. □

With this basic theorem about sumsets proven, we now take a look at restricted sumsets, those being sumsets where a sum is excluded if it satisfies a certain property, normally being the root of a particular polynomial.

Notation (Restricted Sumset)**.** For a polynomial $h(x_0, x_1, \ldots, x_k)$ and subsets $A_0, A_1, \ldots, A_k \subseteq Z_p$ define

$$\oplus_h \sum_{i=0}^{k} A_i = \{a_0+a_1+\ldots+a_k : a_i \in A_i, h(a_0,a_1,\ldots,a_k)\neq 0\}$$

to be the restricted sumset over the A_is with respect to h.

Theorem 3.1.2 (General Restricted Sumset Theorem[1])**.** For a prime p and a polynomial $h(x_0, .., x_k)$ over Z_p and nonempty $A_0, A_1, \ldots, A_k \subseteq Z_p$, define $c_i = |A_i| - 1$ and $m = \sum_{i=0}^{k} c_i - \deg(h)$.
If $[x_0^{c_0} \ldots x_k^{c_k}]((\sum_{i=0}^{k} x_i)^m \cdot h(\mathbf{x})) \neq 0$, then

$$\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geq m + 1 \text{ (consequently m < p).}$$

Proof. Suppose indirectly that the inequality does not hold (and hence $m \geq p$), then we may define $E \subseteq Z_p$ such that E is a multi-set containing m elements and $\oplus_h \sum_{i=0}^{k} A_i \subseteq E$. Let $Q(\mathbf{x}) = h(\mathbf{x}) \prod_{e \in E} \left(\sum_{i=0}^{k} x_i - e \right)$. By our construction we must have that $Q(\mathbf{x}) = 0$ for all $\mathbf{x} \in \prod_{i=0}^{k} A_i$ as either $h(\mathbf{x}) = 0$ or $\sum_{i=0}^{k} x_i \in \oplus_h \sum_{i=0}^{k} A_i \subseteq E$. Furthermore $\deg(Q) = m + \deg(h) = \sum_{i=0}^{k} c_i$ by construction. From this we see $m \geq \sum_{i=0}^{k} c_i$ and hence $[x_0^{c_0} \ldots c_k^{c_k}]Q \neq 0$ (as it is binomial in nature).

Therefore, applying Combinatorial Nullstellenstaz (Theorem 1.2) yields an $\mathbf{a} \in A$ such at $Q(\mathbf{a}) \neq 0$ ↯. Thus $m < p$ and $\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geq m + 1$. □

With this powerful result proven let us now take specific functions for h and prove superior lower bounds where possible. First, we examine the function $h(a_0, \ldots, a_k) = \prod_{0 \leq i < j \leq n} (a_i - a_j)$:

Theorem 3.1.3 (Restricted Sumset Theorem[1])**.** For a prime p, nonempty $A_0, A_1, \ldots, A_k \subseteq Z_p$ with $|A_i| \neq |A_j|$ for any $i \neq j$ and for the h defined above. If $\sum_{i=0}^{k} |A_i| \leq p + \binom{k+2}{2} - 1$, then

$$\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geq \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

A special case of this theorem for only two sets is the following:

Theorem 3.1.4 (Erdős-Heilbronn Conjecture[1])**.** For a prime p and nonempty $A, B \subseteq Z_p$, then $|A \oplus_h B| \geq \min\{p, |A| + |B| - \delta\}$ where $\delta = 3$ for the case $A = B$ and $\delta = 2$ in all other cases.

In order to prove these theorems, let us first state and prove a lemma concerning the coefficient of a particular polynomial:

Lemma 3.1.1. Let $0 \leq c_0, \dots, c_k \in \mathbb{Z}$ and define $m = \sum_{i=0}^k c_i - \binom{k+1}{2}$ (it is trivial that m is nonnegative). Then,

$$[x_0^{c_0} \dots x_k^{c_k}] \left(\left(\sum_{i=0}^{k} x_i \right)^m \prod_{k \geq i > j \geq 0} (x_i - x_j) \right) = \frac{m!}{c_0! c_1! \dots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j) .$$

Provide proof of this lemma based on proof of Ballot problem

With this out of the way, we now prove proposition 2.4:

Proof of Restricted Sumset Theorem . For this proof we will take the aforementioned

$$h(\mathbf{x}) = \prod_{0 \leq i < j \leq k} (x_i - x_j) .$$

Now, let us define $c_i = |A_i| - 1$ and $m = \sum_{i=0}^k c_i - \binom{k+1}{2}$. Rearranging the assumptions of this theorem yields $\sum_{i=0}^k |A_i| - \binom{k+2}{2} + 1 \leq p$ and, applying the trivial combinatorial identity $\binom{k+2}{2} = \binom{k+1}{2} + (k+1)$ yields
$\sum_{i=0}^k c_i - \binom{k+1}{2} + 1 = m + 1 \leq p$ (hence $m < p$). Then

$$[x_0^{c_0} \dots x_k^{c_k}] \left(\left(\sum_{i=0}^{k} x_i \right) h \right) = \frac{m!}{c_0! \dots c_k!} \prod_{0 \leq i < j \leq k} (c_i - c_j) .$$

We know this product to be nonzero modulo p as $c_i \neq c_j$ for $i \neq j$ by construction and $m < p$. Finally, as the coefficient is nonzero and as $\deg(h) = \binom{k+2}{2}$ (as there are $k+2$

possible x_i's and each term of the product will contain two distinct x_i's so there are $\binom{k+2}{2}$ terms each of degree 1), we have $m = \sum_{i=0}^{k} c_i - \deg(h)$. Hence, applying theorem 2.3 yields $\left|\oplus_h \sum_{i=0}^{k} A_i\right| \geq m + 1 = \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1$ by construction. □

Ask grynkiewicz about this as Alons paper says $+\deg(h)$ instead of minus

We conclude this section with the proof of the Erdős-Heilbronn Conjecture:

Proof of Erdős-Heilbronn Conjecture. □

Add proof

3.2 Graphs, Cubes, and Colorings

Now, we present a few combinatorial results of graph theory using the Combinatorial Nullstellensatz. For these proofs assume all graphs are loopless,

Theorem 3.2.1 ([1]). Let p be an odd prime and G ,a graph with $\frac{\sum_{i \in V(G)} d(i)}{e(G)} = d(G) > 2p - 2$ and $\Delta \leq 2p - 1$, we find a p-regular subgraph.

Proof. Let $B = (b_{i,e})_{i \in V(G), e \in E(G)}$ to be the incidence matrix of G, that being, $b_{i,j} = \begin{cases} 1, & i \in e \\ 0, & i \notin e \end{cases}$. For each $e \in E(G)$, let $x_e \in \{0,1\}$ be an associated variable and define

$$\begin{aligned} F &: \{0,1\}^{e(G)} \longrightarrow \mathrm{GF}(p) \\ (x_e)_{e \in E(G)} &\longmapsto F((x_e)_{e \in E(G)}) = \prod_{v \in V} \left[1 - \left(\sum_{e \in E} b_{v,e} x_e\right)^{p-1}\right] - \prod_{e \in E} (1 - x_e) \,. \end{aligned}$$

Then, recall that $\frac{d(G) \cdot v(G)}{2} = e(G)$. Hence, we have $e(G) > \frac{2p-2}{2} v(G) = (p-1)\, v(G)$. And, as the highest order term of the first product has degree $(p-1)$ as each x_e within the sum has degree $p - 1$ and the product over $v(G)$ terms of order $p - 1$ is $v(G)(p-1)$, and the highest order term of the second product is $(-1)^{e(G)-1} \prod_{e \in E(G)} x_e$ of order $e(G)$, hence $\deg(F) = e(G)$. Then, as the highest order term is $\prod_{e \in E(G)} x_e^1$ with each $x_e \in \{0,1\}$, hence as $|\{0,1\}| - 1 = \deg(x_e)$, we see that applying combinatorial nullstellensatz yields an $(x_e)_{e\in E(G)=\mathbf{x}}$ such that $F(\mathbf{x}) \neq 0$ and as $F\left((0)_{e\in E(G)}\right) = 0$, we see $\mathbf{x} \neq (0)_{e\in E(G)}$. Hence, $\prod_{\mathbf{x}}(1 - x_e) = 0$, so we see the first product is nonzero. Then, as $a^{p-1} \equiv 1 \pmod p$ for all $b \neq 0$, we see each $\sum_{e\in E(G)} b_{v,e}x_e = 0$, else the first product would be zero.

Now, let H be the subgraph induced by $E(H) = \{e \in E(G) : x_e = 1\}$ and note that as all terms of the sum $\sum_{e\in E} b_{v,e}x_e$ are either 0 or 1 and as there are precisely 2 $v \in V(G)$ such that $b_{v,e} = 1$ for each $e \in E(G)$, we see $p \mid |\{e \in E(G) : x_e = 1\}$, as p is an odd prime. Then, as $x_e = 1$ for all $e \in E(H)$, we see $\sum_{e\in E(H)} a_{v,e}x_e = \sum_{e\in E(H)} a_{v,e} = d_H(v)$ and as $p \mid e(H) = |\{e \in E(G) : x_e = 1\}|$, we see $p \mid d_H(v)$ for each $v \in V(H)$. Furthermore, as $d(v) < 2p$ for all $v \in H$, we see $d_H(v) = p$ for all $v \in V(H)$. Hence, H is p-regular.

□

Chapter 4

Zeilberger-Bressoud q-Dyson Theorem

The previous results have all been relatively simple applications of the Combinatorial Nullstellensatz. Now, we show its use in a more complex proof. We will construct a generalized laurent polynomial based on the subpower and prove the exact value of its constant term. To begin, recall the subpower,

Notation (Subpower)**.** For a given independent variable q, define

$$(x)_k = (1-x)(1-xq)\left(1-xq^2\right)\dots\left(1-xq^{k-1}\right).$$

For simplicity, define $(x)_0 = 1$.

Now, let us state the Dyson conjecture, though we will not prove it as its result will follow directly from the $q = 1$ case of our main theorem.

Theorem 4.0.1 (Dyson Conjecture)**.**

$$[x_1^0 \dots x_n^0]\left(\prod_{1\le i<j\le n}\left(1-\frac{x_i}{x_j}\right)^{a_i}\right) = \frac{(\sum_{i=1}^n a_i)!}{\prod_{i=1}^n (a_i!)}.$$

A direct generalization of this, the q-Dyson conjecture follows:

Theorem 4.0.2 (q-Dyson Conjecture [3])**.** First, let us define the following polynomial:

$$f_q(\mathbf{x}) = f_q(x_1, x_2, \dots, x_n) \coloneqq \prod_{1\le i<j\le n}\left(\frac{x_i}{x_j}\right)_{a_i}\left(\frac{qx_j}{x_i}\right)_{a_j}.$$

Then,

$$[x_1^0 \dots x_n^0] f_q(\mathbf{x}) = \frac{(q)_{\sum_{i=1}^n a_i}}{\prod_{j=1}^n (q)_{a_j}}.$$

Before we can prove this result, we must examine a related function and prove a result about its coefficients.

Lemma 4.0.1. Let $\mathbb{F}$ be a field and $F \in \mathbb{F}[x_1, \ldots, x_n]$ to be a polynomial of degree $d \leq \sum_{i=1}^{n} d_i$. For arbitrary $A_1, \ldots, A_n \subseteq F$ with $|A_i| = d_i + 1$ for each $1 \leq i \leq n$, we find

$$\left[\prod_{i=1}^{n} x_i^{d_i}\right] F = \sum_{c_1 \in A_1, c_2 \in A_2, \ldots, c_n \in A_n} \frac{F(c_1, c_2, \ldots, c_n)}{\varphi_1'(c_1)\,\varphi_2'(c_2)\ldots\varphi_n'(c_n)}$$

with $\varphi_i(z) = \prod_{a \in A_i}(z - a)$.

Proof. We construct a sequence of polynomials. Let $F_0 = F$ and define F_i as follows. Let $F_i(\mathbf{x}) = \frac{F_{i-1}}{\varphi_i(x_i)}$ in the ring $\mathbb{F}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. We see this construction guarantees $\left[\prod_{i=1}^{n} x_i^{d_i}\right] F_{i-1} = \left[\prod_{i=1}^{n} x_i^{d_i}\right] F_i$ and for all $\mathbf{c} \in \prod_{i=1}^{n} A_i$ we see $F_n(\mathbf{c}) = F(\mathbf{c})$ and $\deg_{x_i}(F_i) \leq d_i$ for all $1 \leq i \leq n$, hence as $\sum_{i=1}^{n} |A_i| > \deg(F)$, we see lagrangian interpolation yields a unique polynomial of the form

$$F_n(\mathbf{x}) = \sum_{\mathbf{c} \in \prod_{i=1}^{n} A_i} F(\mathbf{c}) \prod_{i=1}^{n} \prod_{\gamma \in A_i \setminus c_i} \frac{x_i - \gamma}{c_i - \gamma}..$$

Then, we note for $\varphi_i(z) = \prod_{a \in A_i}(z - a)$, we find $\varphi_i'(z) = \sum_{a_k \in A_i} \prod_{i = a \in A_i \setminus a_k}(z - a)$, and evaluating at a $c_i \in A_i$ yields $\varphi'(c_i) = \prod_{a \in A_i \setminus c_i}(c_i - a)$. Then, we note that $\left[\prod_{i=1}^{n} x_i^{d_i}\right] F_n(\mathbf{x}) = \sum_{c \in \prod_{i=1}^{n} A_i} \frac{F(\mathbf{c})}{\prod_{i=1}^{n} \prod_{\gamma \in A_i \setminus c_i}(c_i - \gamma)} = \frac{F(\mathbf{c})}{\prod_{i=1}^{n} \varphi_i'(c_i)}$. This completes the lemma. □

Proof of q-Dyson Conjecture. First, we note that if $a_i = 0$, then $(x)_{a_i} = (1 - x)$, hence we may omit all of these terms as they will not affect the constant. Hence, we know each (relevant) a_i is a positive integer. Let

$$F(\mathbf{x}) = \prod_{1 \leq i < j \leq n} \left(\prod_{i=0}^{a_i - 1} \left(x_j - x_i q^t\right) \cdot \prod_{t=1}^{a_j} \left(x_i - x_j q^t\right) \right).$$

Denote $\kappa = \frac{1}{\prod_{1\le i<j\le n} x_i^{a_j} x_j^{a_i}}$. Then, we see

$$\begin{aligned} f_q\left(x_1, x_2, \ldots, x_n\right) &= \prod_{1\le i<j\le n} [\prod_{k=1}^{a_i}\left(1-\frac{x_i}{x_j}q^{k-1}\right)\prod_{k=1}^{a_j}\left(1-\frac{x_j}{x_i}q^{k}\right)] \\ &= \prod_{1\le i<j\le n} \frac{1}{x_j^{a_i}x_i^{a_j}}[\prod_{k=1}^{a_i}\left(x_j - x_i q^{k-1}\right)\prod_{i=1}^{a_j}\left(x_i - x_j q^{k}\right)] \\ &= \frac{1}{\prod_{1\le i<j\le n} x_i^{a_j}x_j^{a_i}} \underbrace{\prod_{1\le i<j\le n}[\prod_{k=1}^{a_i}\left(x_j - x_i q^{k-1}\right)\prod_{k=1}^{a_j}\left(x_i - x_j q^{k}\right)]}_{=F(x_1,x_2,\ldots,x_n)} \\ &= \kappa \prod_{1\le i<j\le n} \left(x_j^{a_i} + \beta_i\right)\left(x_i^{a_j} + \beta_j\right) \\ &= \kappa \prod_{1\le i<j\le n} \left(x_j^{a_i}x_i^{a_j} + \beta_{ij}\right) \\ &= c\kappa\left(\prod_{1\le i<j\le n} x_j^{a_i}x_i^{a_j}\right) + \beta, \end{aligned}$$

where $\beta_i, \beta_j, \beta_{ij}, \beta$ are all of the lower order terms from their respective product. We see the first term is simply a constant, and we see as the exponent of x_i will take on all values, a_k, except a_i and similarly, the exponent of x_j will take on all values except a_j. Hence, we find [1] $f_q\left(\mathbf{x}\right) = \left[\prod_{i=1}^{n} x_i^{\sum_{k=1}^{n} a_k - a_i}\right] F\left(\mathbf{x}\right)$.

Now, we define $\sum_{i=1}^{n} a_i = \sigma$, $A_i = \{1, q, \ldots, q^{\sigma - a_i}\}$ and a sequence $\sigma_0 = 0$, $\sigma_i = \sum_{j=1}^{i-1} a_j$ for $2 \le i \le n+1$. It is clear $|A_i| = \sigma - a_i + 1$ and $\sigma_{n+1} = \sigma$. Now, we aim to prove that for $\mathbf{c} = (c_1, \ldots, c_n) \in \prod_{i=1}^{n} A_i$, we have $F\left(\mathbf{c}\right) = 0$ unless $c_i = q^{\sigma_i}$ for each $1 \le i \le n$.

We will suppose a contradiction, that is there exists a $(c_1, c_2, \ldots, c_n) = \mathbf{c} \in \prod_{i=1}^{n} A_i$ such that $F\left(\mathbf{c}\right) \neq 0$ for $c_i = q^{\alpha_i}$ where $0 \le \alpha_i \le \sigma - a_i$. Then, we see for a pair $j > i$, we have $\alpha_j - \alpha_i \ge a_i$, in particular every pair α_j, α_i with $i \neq j$ is distinct. Then, we see their is a unique ordering π such that $\alpha_{\pi(1)} < \alpha_{\pi(2)} < \ldots < \alpha_{\pi(n)}$. Then, summing over the inequality $\alpha_{\pi(i+1)} - \alpha_{\pi(i)} \ge a_{\pi(i)}$

for $1 \leq i \leq n-1$ yields

$$\begin{aligned} \left(\alpha_{\pi(_n)} - \alpha_{\pi(n-1)}\right) + \left(\alpha_{\pi(n-1)} - \alpha_{\pi(n-2)}\right) + \ldots + \left(\alpha_{\pi(2)} - \alpha_{\pi(1)}\right) &= \alpha_{\pi(n)} - \alpha_{\pi(1)} \\ &\geq \sum_{i=1}^{n-1} a_{\pi(i)} \\ &= \sigma - a_{\pi(n)}. \end{aligned}$$

Then, as $\alpha_{\pi(1)} \geq 0$ and $\alpha_{\pi(n)} \leq \sigma - a_{\pi(n)}$ by the original inequality, we find equality must hold, hence

$$\alpha_{\pi(n)} - \alpha_{\pi(1)} = \sigma - a_{\pi(n)} = \sigma_n.$$

We see this summation works over $k < n-1$ terms as well, so $\alpha_{\pi(k)} = \sigma_k$ hence π must be the identity permutation and we see $\alpha_k = \sum_{i=1}^{k-1} a_i = \sigma_k$ for all $1 \leq k \leq n$. $\lightning$. Hence, we see $F(\mathbf{c}) = 0$ unless each $c_i = q^{\sigma_i}$, so the constant

$$[1]\, f_q = \frac{F\left(q^{\sigma_1}, \ldots, q^{\sigma_n}\right)}{\varphi_1'\left(q^{\sigma_1}\right) \ldots \varphi_n'\left(q^{\sigma_n}\right)}$$

by the lemma.

Now, denote $\tau_i = \binom{\sigma_i}{2} + \sigma_i\left(\sigma - \sigma_i + 1\right)$ and we derive a subpower form of $\varphi_i'\left(q^{\sigma_i}\right)$.

Then we see

$$\begin{aligned}
\varphi_i'\left(q^{\sigma_i}\right) &= \prod_{\substack{0\leq t\leq \sigma-a_i \\ t\neq\sigma_i}} \left(q^{\sigma_i}-q^t\right) \\
&= \prod_{t=0}^{\sigma_i-1}\left(q^{\sigma_i}-q^t\right)\prod_{t=\sigma_i+1}^{\sigma-a_i}\left(q^{\sigma_i}-q^t\right) \\
&= \prod_{t=0}^{\sigma_i-1}(-q)^t\left(1-q^{\sigma_i-t}\right)\prod_{t=1}^{\sigma-\sigma_i-a_i} q^{\sigma_i}\left(1-q^t\right) \\
&= (-1)^{\sigma_i}\cdot \underbrace{\prod_{i=1}^{\sigma_i-1} q^t}_{=q^{\sum_{i=1}^{\sigma_i-1}1}=q^{\frac{\sigma_i(\sigma_i-1)}{2}}=q^{\binom{\sigma_i}{2}}} \cdot \underbrace{\prod_{i=0}^{\sigma_i-1}(1-q^{\sigma_i-t})}_{=(q)_{\sigma_i}}\cdot \underbrace{\prod_{i=1}^{\sigma-\sigma_{i+1}} q^{\sigma_i}}_{=q^{\sigma_i(\sigma-\sigma_{i+1})}} \cdot \underbrace{\prod_{i=1}^{\sigma-\sigma_{i+1}}\left(1-q^t\right)}_{=(q)_{\sigma-\sigma_{i+1}}} \\
&= (-1)^{\sigma_i} q^{\binom{\sigma_i}{2}+\sigma_i(\sigma-\sigma_{i+1})}(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}} \\
&= (-1)^{\sigma_i} q^{\tau_i}(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}}.
\end{aligned}$$

Similarly by double counting the terms and performing simple manipulations, we find $F\left(q^{\sigma_1},\ldots,q^{\sigma_n}\right)$ in a subpower form. First, note that we can write a partial sequence from $(\sigma_j-\sigma_i-a_i)=(\sigma_j-\sigma_{i+1})$ to $(\sigma_j-\sigma_i)$ as

$$\prod_{t=0}^{a_i-1}\left(1-q^{\sigma_j-\sigma_i-t}\right)=\frac{\prod_{t=1}^{\sigma_j-\sigma_i}\left(1-q^t\right)}{\prod_{t=1}^{\sigma_j-\sigma_i-a_i}\left(1-q^t\right)}=\frac{\prod_{t=1}^{\sigma_j-\sigma_i}\left(1-q^t\right)}{\prod_{t=1}^{\sigma_j-\sigma_{i+1}}\left(1-q^t\right)}=\frac{(q)_{\sigma_j-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}}.$$

Similarly, we find a partial sequence from $(\sigma_j-\sigma_i)$ to $(\sigma_j+a_j-\sigma_i)=(\sigma_{j+1}-\sigma_i)$ to be

$$\prod_{t=1}^{a_j}\left(1-q^{\sigma_j-\sigma_i+t}\right)=\frac{\prod_{t=1}^{\sigma_j+a_j-\sigma_i}\left(1-q^t\right)}{\prod_{t=1}^{\sigma_j-\sigma_i}\left(1-q^t\right)}=\frac{\prod_{t=1}^{\sigma_{j+1}-\sigma_i}\left(1-q^t\right)}{\prod_{t=1}^{\sigma_j-\sigma_i}\left(1-q^t\right)}=\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_i}}.$$

Now, let $u=\sum_{i=1}^n (n-i)\,a_i$ and $v=\sum_{i=1}^n\left[(n-i)\left(a_i+\sigma_i+\binom{a_i}{2}\right)+\sigma_i\left(\sigma-\sigma_{i+1}\right)\right]$

and we see

$$
\begin{aligned}
F\left(q^{\sigma_1}, q^{\sigma_2}, \ldots, q^{\sigma_n}\right) &= \prod_{1 \le i < j \le n} \left(\prod_{t=0}^{a_i - 1} \left(q^{\sigma_j} - q^{\sigma_i} q^t\right) \cdot \prod_{t=1}^{a_j} \left(q^{\sigma_i} - q^{\sigma_j} q^t\right) \right) \\
&= \prod_{1 \le i < j \le n} (-1)^{a_i} \left(\underbrace{\prod_{t=0}^{a_i - 1} q^{\sigma_i + t}}_{= q^{a_i \sigma_i} q^{\binom{a_i}{2}}} \underbrace{\prod_{t=0}^{a_i - 1} (1 - q^{\sigma_j - \sigma_i - t}) \cdot}_{= \frac{(q)_{\sigma_j - \sigma_i}}{(q)_{\sigma_j - \sigma_{i+1}}}} \underbrace{\prod_{t=1}^{a_j} q^{\sigma_i}}_{= q^{\sigma_i (\sigma - \sigma_{i+1})}} \underbrace{\prod_{t=1}^{a_j} \left(1 - q^{\sigma_j - \sigma_i + t}\right)}_{= \frac{(q)_{\sigma_{j+1} - \sigma_i}}{(q)_{\sigma_j - \sigma_i}}} \right) \\
&= (-1)^{\sum_{i=1}^n (n-i) a_i} \, q^{\sum_{i=1}^n \left[(n-i)(a_i \sigma_i + \binom{a_i}{2}) + \sigma_i (\sigma - \sigma_{i+1}) \right]} \prod_{1 \le i < j \le n} \frac{(q)_{\sigma_{j+1} - \sigma_i}}{(q)_{\sigma_j - \sigma_{i+1}}} \\
&= (-1)^u \, q^v \frac{\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (q)_{\sigma_{j+1} - \sigma_i}}{\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (q)_{\sigma_j - \sigma_{i+1}}} \\
&= (-1)^u \, q^v \frac{\prod_{i=1}^{n-1} \prod_{j=i+2}^{n+1} (q)_{\sigma_j - \sigma_i}}{\prod_{i=2}^{n} \prod_{j=i}^{n} (q)_{\sigma_j - \sigma_i}} \\
&= (-1)^u \, q^v \frac{\prod_{j=3}^{n+1} (q)_{\sigma_j - \sigma_1} \, (\prod_{i=2}^{n-1} \prod_{j=i+2}^{n} (q)_{\sigma_j - \sigma_i})(\prod_{i=2}^{n-1} (q)_{\sigma_{n+1} - \sigma_i})}{(\prod_{i=2}^{n-1} \prod_{j=i+2}^{n} (q)_{\sigma_j - \sigma_i})(\prod_{i=2}^{n-1} \prod_{j=i}^{i+1} (q)_{\sigma_j - \sigma_i})} \\
&= (-1)^u \, q^v \frac{\prod_{i=2}^{n-1} (q)_{\sigma - \sigma_i} \prod_{j=3}^{n+1} (q)_{\sigma_j - \sigma_1}}{\prod_{i=2}^{n-1} (q)_{\sigma_{i+1} - \sigma_i}} \cdot \frac{(q)_{\sigma_2 - \sigma_1}}{(q)_{\sigma_2 - \sigma_1}} \cdot \frac{(q)_{\sigma - \sigma_n}}{(q)_{\sigma - \sigma_n}} \underbrace{(q)_{\sigma_1 - \sigma_1}}_{1} \\
&= (-1)^u \, q^v \frac{\prod_{i=2}^{n} (q)_{\sigma - \sigma_i} \cdot (q)_{\sigma - \sigma_1} \cdot \prod_{i=1}^{n} (q)_{\sigma_i}}{\prod_{i=1}^{n} (q)_{\sigma_{i+1} - \sigma_i}} \\
&= (-1)^u \, q^v \prod_{i=1}^{n} \frac{(q)_{\sigma_i} \, (q)_{\sigma - \sigma_i}}{(q)_{\sigma_{i+1} - \sigma_i}}.
\end{aligned}
$$

From here, we see

$$\begin{aligned}\sum_{i=1}^{n}(n-i)\,a_i &= (n-1)\,a_1+(n-2)\,a_2+\ldots+0a_n\\ &= \sum_{i=1}^{n-1}a_i+\sum_{i=1}^{n-2}a_i+\ldots+\sum_{i=1}^{1}a_i+\underbrace{\sum_{i=1}^{0}a_i}_{0}\\ &= \sigma_n+\sigma_{n-1}+\ldots+\sigma_2+\underbrace{\sigma_1}_{0}\\ &= \sum_{i=1}^{n}\sigma_i\end{aligned}$$

.

Hence, $u=\sum_{i=1}^{n}\sigma_i$ and the powers of -1 will vanish. Similarly, we see by induction that the powers of q vanish, that is $\sum_{i=1}^{n}(n-i)\left(a_i\sigma_i+\binom{a_i}{2}\right)=\sum_{i=1}^{n}\binom{\sigma_i}{2}$. Now note that for $j=0$, we have $\sum_{i=1}^{0}(0-i)\left(a_i\sigma_i+\binom{a_i}{2}\right)=\sum_{i=1}^{0}\binom{\sigma_i}{2}=0$. Then, assuming the case j to be true, we see

Figure out induction

Assembling our results yields

$$\begin{aligned}\text{[1] } f_q(\mathbf{x}) = \frac{F\left(q^{\sigma_1},\ldots,q^{\sigma_n}\right)}{\varphi_1'\left(q^{\sigma_1}\right)\ldots\varphi_n'\left(q^{\sigma_n}\right)} &= \prod_{i=1}^{n}\frac{(q)_{\sigma_i}(q)_{\sigma-\sigma_i}}{(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}}(q)_{\sigma_{i+1}-\sigma_i}}\\ &= \frac{(q)_{\sigma-\sigma_1}}{\prod_{i=1}^{n}(q)_{\sigma_{i+1}-\sigma_i}}\\ &= \frac{(q)_{\sigma}}{\prod_{i=1}^{n}(q)_{a_i}}\\ &= \frac{(q)_{a_1+a_2+\ldots+a_n}}{(q)_{a_1}\ldots(q)_{a_n}}.\end{aligned}$$

□

Chapter 5

Chevalley-Warning Theorem and Kemnitz Conjecture

Move Chevalley-Warning to its own section and proved 1-2 more statements and proofs on sumsets

Our first major theorem of this section concerns the theorem of Chevalley and Warning which declares the conditions under which a certain nontrivial solution to a polynomial in a finite field of characteristic p can exist:

Theorem 5.0.1 (Chevalley-Warning Theorem)**.** Let F be a finite field of characteristic p and let $f_1, f_2, \ldots, f_k \in F[x_1, x_2, \ldots, x_n]$ be polynomials and N to be the number of points $\mathbf{x} \in F^n$ such that $f_1(\mathbf{x}) = \ldots = f_k(\mathbf{x}) = 0$. If $\sum_{i=1}^{k} \deg(f_i) < n$, then $N \equiv 0 (\text{mod } p)$.

In order to provide a proof of this statement, let us first state and prove the following lemma:

Lemma 5.0.1 (Lemma)**.** Let F be a finite field and $k_1, k_2, \ldots, k_n \geq 0$ such that $\min_{1\leq i\leq n} k_i \leq |F| - 2$. Then, $\sum_{x_1,x_2,\ldots,x_n \in F} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = 0$. (Note: if a 0^0 occurs in the expressions it will be treated as a 1).

Proof. Assume without loss of generality that $k_1 < |F| - 1$. Then, by factoring out a $x_1^{k_1}$ from each term of the sum and grouping all such x_1's, we have $\sum_{x_1,x_2,\ldots,x_n \in F} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = \left(\sum_{x_1 \in F} x_1^{k_1}\right) \sum_{x_2,\ldots,x_n \in F} x_2^{k_2} \ldots x_n^{k_n}$, hence we must only show that $\sum_{x_1 \in F} x_1^{k_1} = 0$. Suppose $k_1 = 0$, then $\sum_{x_1 \in F} x_1^{k_1} = |F|$ and, since p divides $|F|$ we see the case $k_1 = 0$ is trivially true. Now, let $\omega \in F^{\times}$ be a generator of $F^{\times}$. Then, we have that

$$\sum_{x_1 \in F} x_1^{k_1} = \sum_{x_1 \in F^{\times}} x_1^{k_1} = \sum_{x_1 \in F^{\times}} (\omega x)^{k_1} = \omega^{k_1} \sum_{x_1 \in F^{\times}} x_1^{k_1} = \omega^{k_1} \sum_{x_1 \in F} x_1^{k_1}.$$

Taking the difference of the first and last terms of the above equality yields $\left(\omega^{k_1} - 1\right)\left(\sum_{x_1 \in F} x_1^{k_1}\right) = 0$, so we must have either the sum is 0 or $\omega^{k_1} - 1 = 0$.

However, as ω is a generator of the cyclic group $F^{\times}$, we may only have that $\omega^{k_1} = 1$ if $k_1 \equiv -1 \pmod{|F|}$. But, as $0 < k_1 < |F| - 1$ this case cannot occur, hence we see $\sum_{x_1 \in F} x_1^{k_1} = 0$, so the lemma is proven. □

Proof of Chevalley-Warning Theorem. Recalling that $x^{|F|} = x$ (and thus $x^{|F|-1} = 1$ for nonzero x). Then, define

$$M = \sum_{\mathbf{x} \in F^n} \prod_{i=1}^{k} \left(1 - f_i \left(\mathbf{x}\right)^{|F|-1}\right).$$

We see, by the earlier proposition, that a term of the sum will be 1 if and only if **x** is a solution to the system $f_1, f_2, \ldots, f_k$, else it will be 0. Furthermore, it is clear by the construction that M will be exactly equal to the number of solutions to our system $f_1, \ldots, f_k$, and hence it precisely N.

Now, let us define the product from our construction to be a polynomial g, that is $g\left(\mathbf{x}\right) = \prod_{i=1}^{k} \left(1 - f_i \left(\mathbf{x}\right)^{|F|-1}\right)$. Then, repeatedly applying the substitution $x_j^{|F|} \to x_j$ to g yields a polynomial $\overline{g} = g$ for all $\mathbf{x} \in F^n$. Furthermore, $\deg_{x_j}\left(\overline{g}\right) \leq |F| - 1$ for $1 \leq j \leq n$(This is clear as , if it were not we would be able to apply the substitution once again). Then, substituting $\overline{g}$ in place of g yields

$$M = \sum_{\mathbf{x} \in F^n} \overline{g}\left(\mathbf{x}\right).$$

Then, applying our lemma, we see that all monomials with degree $|F| - 2$ or less will equal 0 and hence the only possible nonzero terms of $\overline{g}$ are those of the form $\prod_{i=1}^{n} x_i^{|F|-1}$. Expanding the product, we see that such a monomial would be of degree $n\left(|F| - 1\right)$, however as $\deg f_i^{|F|-1} = \left(|F| - 1\right) \deg\left(f_i\right)$, we see that $\deg\left(g\right) \leq \left(|F| - 1\right) \sum_{i=1}^{k} f_i < n\left(|F| - 1\right)$ by construction. Consequently, any such monomial of $\overline{g}$ (and hence g) will have a zero coefficient, and thus $M = N \equiv 0 \pmod{p}$. □

This theorem allows us to prove certain constraints (and in the case of prime p, the exact value) on the size of the davenport constant for a certain group. This result is too advanced for now, but we will return to it later. Next, let us examine theorems concerning sumsets such as the Cauchy-Davenport Theorem and the Erdős-Heilbronn conjecture on the lower bound of the size of sumsets.

REFERENCES

[1] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8(1-2):7–29, 1999.

[2] David J. Grynkiewicz. *The Polynomial Method: The Erdos:Heilbronn Conjecture*, volume 30. Springer, 2013.

[3] Gyula Károlyi and Zoltán Nagy. A simple proof of the zeilberger–bressoud q-dyson theorem. *Proceedings of the American Mathematical Society*, 142(9):3007–3011, Sep 2014.